
BEFORE THE
FEDERAL COMMUNICATIONS COMMISSION
WASHINGTON, D.C. 20554

RECEIVED
FEB 11 1998
FEDERAL COMMUNICATIONS COMMISSION
OFFICE OF THE SECRETARY

IN THE MATTER OF:

Communications Assistance
For Law Enforcement Act
(CALEA)

)
)
)
)
)

CC Docket No. 97-213

REPLY COMMENTS OF SBC COMMUNICATIONS INC.

JAMES D. ELLIS
ROBERT M. LYNCH
DURWARD D. DUPRE
LUCILLE M. MATES
FRANK C. MAGILL

ATTORNEYS FOR
SBC COMMUNICATIONS INC.
175 E. Houston
Room 4-H-40
San Antonio, Texas 78205
(210) 351-5575

February 11, 1998

TABLE OF CONTENTS

	Page
SUMMARY	ii
Introduction	1
I. Carriers Subject to CALEA	1
II. Review of Validity of Court Orders by Carriers	2
III. Security and Recordkeeping Policies	4
IV. FCC Involvement in the Industry Standards Process	7
V. Reasonable Achievability and Extensions of Compliance Deadlines	8
VI. Conclusion	10

SUMMARY

Congress authorized the Commission to prescribe such rules *as are necessary* to implement the requirements of CALEA. SBC endorses strict compliance with this statutory limitation. The rules that are necessary and adopted by the Commission, however, should apply to all entities offering telecommunications services to the extent of such offering. Entities such as grocery stores and pharmacies that sell prepaid calling cards, which are used as a billing mechanism, do not offer telecommunications services and should not be subject to CALEA.

SBC agrees with the FBI that CALEA does not vest carriers with either the authority or legal accountability for determining the validity of court orders or other lawful authorization. But, that is a different issue from whether CALEA requires carriers to enable surveillance in ways not previously available to law enforcement, which is contrary to the stated intent of CALEA. While carriers are responsible to provide assistance strictly in accordance with the terms of a facially valid order or authorization, the industry does not share the FBI's conviction that carriers will be exempt from liability for implementing an intercept that would enable surveillance in ways heretofore not available to law enforcement unless the order or authorization specifies surveillance in such manner.

The comments filed in response to the NPRM overwhelmingly demonstrate that there is no legitimate ground to justify the massive regulatory structure proposed for carriers' internal policies and procedures. The FBI's overstated and speculative narrative on the existence and scope of alleged impediments to effective electronic

surveillance reveals that there is no serious problem with carriers' current methods of ensuring security and record keeping. Thus, without a clear showing of necessity, the FCC should not adopt its proposed rules, much less the more burdensome and expensive regulation that the FBI suggests, which even the FBI recognizes can only impede the timeliness of interceptions. Moreover, SBC agrees with the Center for Democracy and Technology that Section 105 of CALEA was intended to protect the security of central office-based, mechanized surveillance technology from unauthorized activation or access, not to engender the proposed thicket of bureaucracy.

The FBI's continued insistence on expanding its electronic surveillance capabilities by requiring "punch list" capabilities (which it now tries to obtain through its "back door" approach of trading its support for deadline extensions for manufacturers' agreement to include such capabilities in their designs) continues to lend uncertainty to the standards for implementing CALEA. Consequently, SBC suggests that it is time for the FCC to take an active role in establishing compliance standards for carriers. The FCC should do so by responding to the CTIA Petition immediately.

The Commission should adopt AT&T's recommendation that filing a petition for determination of reasonable achievable should automatically toll the applicable compliance deadline until the FCC makes its determination on the petition. Moreover, the comments provide the Commission with a clear record to support its extension of the CALEA compliance deadlines until equipment needed to comply with CALEA is commercially available and can be deployed by carriers.

**BEFORE THE
FEDERAL COMMUNICATIONS COMMISSION
WASHINGTON, D.C. 20554**

IN THE MATTER OF

**Communications Assistance
For Law Enforcement Act
(CALEA)**

)
)
)
)
)

CC Docket No. 97-213

REPLY COMMENTS OF SBC COMMUNICATIONS INC.

Introduction

SBC hereby respectfully submits its Reply to the Comments filed on or before December 12, 1997, in the above-captioned docket. The following Reply focuses on those issues addressed in SBC's initial Comments which appeared to generate the most discussion among the other filing parties, and/or which are of the most significance, in SBC's opinion, to the stated purposes of this proceeding. The Reply is organized by issue or issue group, as appropriate, for ease of reference.

I. Carriers Subject to CALEA

SBC reiterates its previously stated position that all entities offering telecommunications services to the public should be, and must be, deemed subject to CALEA's requirements to the extent of such offering.

The FBI somewhat confuses the issue with respect to CALEA's applicability to resellers when it refers, in its Paragraph 26, to "resellers with prepaid calling card or other similar services." Prepaid calling cards themselves should not be at issue here: the key point the FBI makes, with which SBC agrees, is that resellers of telecommunications services in general should be subject to CALEA. A prepaid calling card is not a telecommunications service but rather a billing mechanism, in fact, not unlike secured Visa or MasterCard credit cards. CALEA only covers the "equipment, facilities, or services that provide a customer or subscriber with the ability to originate, terminate, or direct communications ..." (Sec 103(a)). A prepaid calling card does not provide a subscriber with any of these capabilities. Thus, whether or not they offer prepaid calling cards, all resellers of telecommunications services are covered; conversely, an agent who sells prepaid calling cards but does not actually provide dial tone to customers, should not be covered by CALEA. In the latter case, the carrier whose network is ultimately used to carry a call paid by a prepaid calling card will already be covered by CALEA.

II. Review of Validity of Court Orders by Carriers

SBC agrees generally with the FBI's arguments, in its Paragraphs 31-36, to the effect that CALEA does not vest carriers with either the primary authority or the legal accountability for determining the underlying validity of court orders

or other lawful authorizations under the electronic surveillance laws.¹ Carriers have never had, and do not now desire, such authority and accountability, and should remain protected from liability under both CALEA and the surveillance statutes to the extent they implement facially valid court orders or certifications in good faith. This does not change the fact, of course, that carriers are charged by CALEA with responsibility for determining in each instance that a given court order or other authorization in fact is valid on its face, and for ensuring that whatever assistance is provided to law enforcement pursuant thereto is strictly in accordance with the terms of the order or authorization and with the enabling statutes, including but not limited to CALEA.

Thus, it is important to note that a carrier's legal accountability in relation to the inclusion of the FBI's "punch list" of advanced surveillance functions in industry standards and/or carrier networks is entirely different from, although clearly related to, a carrier's duty to render assistance to law enforcement in compliance with a specific order or request. The industry does not share the FBI's conviction that carriers will be exempted from any liability for implementing an intercept that would enable surveillance to occur in ways heretofore not available to law enforcement, in light of the Congressional intent that CALEA not expand surveillance capabilities beyond those lawfully available prior to its enactment. It is by no means clear that the "good faith reliance" provisions of 18 U.S.C. §2518 and similar laws would offer a carrier any protection from liability

¹ As stated in our initial Comments, however, SBC does not agree that Section 229(b)(1) refers to a carrier's internal authorization procedures.

where “punch list” functions are made available in connection with surveillance orders or requests *that do not themselves specify the use of such functions to intercept the communications of unnamed persons*. The FBI has refused SBC’s suggestion that law enforcement could satisfy carriers’ concerns by drafting court affidavits and certifications to include such specifications, *i.e.*, if the particular advanced functionality, such as continued monitoring of three-way calls after the named subject drops off, were to be specified as necessary in the court order. In essence, then, the FBI and Justice Department insist that carriers accept without argument the government’s bare conclusion that the “punch list” is permitted or even mandated by CALEA, and that its deployment and use would not increase carriers’ liability risks in suits by surveillance targets. At the same time, the government refuses to consider agreeing to support or defend carriers if such litigation does arise. Under these circumstances, no prudent carrier could reasonably be expected willingly to take such risks.

III. Security and Recordkeeping Policies

As the overwhelming weight of the comments from carriers demonstrates, there is simply no need for a complex, burdensome and expensive set of regulations governing carriers’ handling of internal corporate matters such as security, personnel policies, record keeping, authorization and employee designation in connection with electronic surveillance. Every established carrier, including SBC, already has in place policies that more than adequately ensure compliance with CALEA, with the pre-existing confidentiality mandates of the

electronic surveillance statutes and similar state laws, and with the demands of the rules of evidence for appropriate implementation, conduct and record keeping pursuant to court orders and other lawful surveillance authorizations. It is perhaps not surprising, then, that no evidence has been presented to Congress or to the FCC even remotely suggesting that a serious problem exists in the industry with respect to these matters.

Nevertheless, the FBI devotes more than a fourth of its 44-page Comments (Paragraphs 36 through 72, at pages 18 to 32) to advocating the imposition of what amounts to nearly total Federal control of carriers' personnel, internal security, surveillance implementation and record keeping policies and procedures. Such a proposal is particularly questionable in light of the FBI's recognition of the fact that civil liability already awaits any carrier whose policies do not adequately protect against unlawful surveillance and preserve the confidentiality of lawfully authorized intercepts. SBC again points out that Section 301 of CALEA (Section 229 of the Communications Act) only requires the imposition of *such rules as are necessary* to implement CALEA Section 105. In support of its claim of need for its proposed rules, the FBI offers only rhetoric about the importance of electronic surveillance to the public interest in law enforcement, coupled with dire predictions as to what *might* happen if carriers suddenly stopped acting responsibly. It cannot be over-emphasized that there are no facts to support such speculation, and therefore no basis exists for such intrusive regulations as the FBI and the FCC propose. Indeed, their adoption by

the FCC would be arbitrary at best, would clearly exceed the statutory mandate, and most likely would be subjected to legal challenge on these grounds.²

Even aside from the lack of any proof of need for a new web of costly administrative regulations, the FBI's advocacy thereof is difficult to reconcile with its recognition that "the more cumbersome a carrier's implementation procedure, the greater the likelihood that investigations will be hampered by unnecessary delays", (FBI, Para. 64), and with its statement that "Law Enforcement wishes to ensure that the paperwork burden is never permitted to impede the timeliness with which intercept requests are implemented." (Id.) The FBI's suggested

² The FCC should also take note of the FBI's tendency to overstate both the existence and the scope of alleged impediments to effective electronic surveillance. SBC does not here seek to revisit the underlying rationale for enactment of CALEA, nor does SBC believe that such a discussion is germane to the issues raised by the NPRM. Nevertheless, for whatever reason, the FBI felt the need to devote part of its Comments to its views in this regard, and SBC believes the Commission should have the benefit of other views as well. For example, in its Footnote 17, after several pages of text suggesting that the very fabric of law enforcement effectiveness is threatened by the changing technology of telecommunications, the FBI offers in support Mr. Freeh's Congressional testimony that "...over the last *decade*, it is conservatively estimated that several hundred electronic surveillance and pen register and trap and trace court orders have been frustrated, in whole or in part, by various technological impediments...." (Emphasis added.) When considered in light of the total number of surveillance orders, however, these estimates illustrate that the real magnitude of the problem is much smaller than the FBI maintains. As noted in its original Comments, SBC's two largest subsidiaries alone (Pacific Bell and Southwestern Bell) process approximately 5,000 surveillance orders per year. If we extrapolate therefrom a reasonable estimate of 25,000 to 35,000 such orders annually across the industry, by assuming that five RBOC's each conduct the same approximate number of Title III, pen register and trap and trace interceptions annually, plus another 5,000 to represent the rest of the industry, and multiply the annual total by ten years to match Mr. Freeh's chosen frame of reference, we find that *only "several hundred" out of 250,000 to 350,000 surveillance orders* suffered any "technological impediments". Even if we give Mr. Freeh's numbers the benefit of multiplying them several times, to assume 2,500 to 3,500 orders might have been affected over that time, law enforcement's claimed problems occurred in only *one percent* of all cases. All of this is simply to emphasize that, before imposing costly regulatory and administrative burdens on carriers under CALEA, the FCC should require the FBI to put forward verifiable facts instead of rank speculation, and those facts should indicate the existence of real problems justifying the financial and productivity costs of the proposed solution.

scheme, applied to each of the thousands of intercepts the larger carriers conduct annually, would virtually guarantee unwarranted delays in many cases.

Finally, SBC agrees with the Center for Democracy and Technology (CDT) and its co-commenters that both the FCC and the FBI have seriously misinterpreted the intent of Section 105. As CDT points out, the legislative history clarifies that Section 105 was intended primarily to protect the security of central office-based, mechanized surveillance technology from unauthorized activation or access, whether from “inside” or by means of intrusions originating outside the carrier’s premises. Section 105 and Section 301 clearly were *not* intended to spawn a huge regulatory machine to micromanage a significant portion of the security and personnel practices of every company in the industry. To the extent that the statutory mandate requires any FCC oversight in this area, the same can and should be discharged by simply confirming that carriers’ existing controls and practices are reasonably effective in assuring compliance with applicable laws. Unless and until proof to the contrary is presented, any regulations such as proposed by the FCC would exceed the FCC’s statutory authority, and would be arbitrary and capricious under applicable standards of judicial review.

IV. FCC Involvement in the Industry Standards Process

SBC agrees that the FCC should defer involvement in industry standards for CALEA compliance, at least in *this* proceeding. While it is clear that CALEA does not exempt industry from the duty to comply with CALEA simply because

no standard is formulated, it is equally clear that the “safe harbor” CALEA provides for carriers who comply with such a standard is effective unless and until the FCC rules otherwise in response to the petition of CTIA or some other interested party. An interim standard, SP3580A, now has been adopted. In view of these facts, SBC objects strongly to the Government’s current strategy of conditioning support for compliance deadline extensions (See Section V, *infra*) on agreements between the FBI and manufacturers regarding inclusion of the FBI’s “punch list” capabilities in specific switch platforms or non-switch-based CALEA “solutions”.³ This “back door” approach by the FBI to obtaining the controversial capabilities it desires is a clear violation of §103(b) of CALEA. If the FBI believes that CALEA permits or mandates inclusion of the “punch list” in the industry standard if the “safe harbor” is to apply, then it must make its case before the Commission. Since a petition from CTIA already is on file requesting FCC review of what is now SP3580A, SBC urges the Commission to take up that petition as soon as possible.

V. Reasonable Achievability and Extensions of Compliance Deadlines

SBC agrees with the suggestion of AT&T (AT&T, p. 22) that the filing of a petition for determination of reasonable achievability under CALEA Section 107 should automatically toll the applicable compliance deadline until the

³ Letter of Janet Reno, Attorney General, to Mr. Matthew J. Flanigan, President, Telecommunications Industry Association, January 23, 1998; Letter of Stephen R. Colgate, Assistant Attorney General for Administration, to Geoffrey Feiss, Director-State Relations, United States Telephone Association, February 2, 1998. Copies of these letters are attached to these Reply Comments as Appendix 1 and 2, respectively.

Commission makes a determination and formally acts on the petition. SBC also agrees that, if compliance is determined to be reasonably achievable, any applicable deadline must be further extended to permit a reasonable time for implementation by the carrier.

SBC urges the Commission to note the overwhelming weight of the comments in favor of liberal extensions of the CALEA compliance deadlines because of the lack of commercially available software and/or hardware necessary to achieve compliance, and to note particularly the fact that, in two major ways, the government itself is partially responsible for this state of affairs: First, by failing to issue any meaningful notice of capacity requirements for over three years since enactment of CALEA, and second, by obstructing the standard-setting process due to its insistence that the standards include the “punch list”. Network planners and engineers simply cannot take any substantial steps toward full CALEA compliance until final and realistic capacity requirements are made known, and until the FBI-created cloud over the existing interim standard is cleared away by an FCC ruling on CTIA’s petition.

SBC has difficulty understanding exactly what the FBI means when it asks the FCC to “present its determinations [regarding reasonably achievable network modifications] in terms of dollar amounts.” (FBI, Para. 95). Although it may well be, as the FBI suggests, that in some instances the circumstances could dictate a “partial” determination of “reasonably achievable” based on a division of costs between a carrier and the government, SBC cautions against any assumption that such an analysis will be applicable in all cases where a carrier or other party

petitions the Commission for a “reasonably achievable” determination. CALEA requires that many factors other than cost alone be considered in such determinations. Applying those factors properly, it may well be that a particular modification or set of modifications would be found not to be reasonably achievable at any cost. In line with this reasoning, the FBI’s proposal (Para. 94) that all petitions be accompanied by an estimate of “the reasonable costs directly associated with the modifications under consideration” should not be adopted for all cases. Of course, where the gravamen of the petition is a carrier’s contention that a modification is not reasonably achievable due to its cost, then the FBI’s suggestion makes sense. Even so, SBC urges the Commission to be mindful of the fact that, as demonstrated by its CALEA cost recovery regulations and industry comments thereon, the FBI’s view of what constitutes “reasonable” costs is substantially different from the view of SBC and other carriers, and is not necessarily representative of Congressional intent.

VI. Conclusion

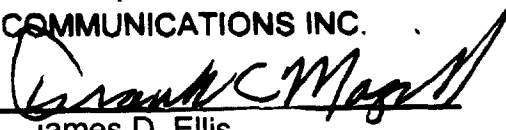
The record demonstrates overwhelmingly that the Commission has no legitimate grounds for adopting the massive regulatory structure proposed in the NPRM regarding carriers’ internal policies and procedures. The record is similarly clear in showing that an extension of the CALEA capability compliance deadline for at least two years, to October of 2000, is warranted and should be granted forthwith. Finally, the record shows that prompt FCC action on the pending CTIA petition is necessary in order to resolve the legal issues arising

from the FBI's continued insistence on having its "punch list" of legally controversial surveillance capabilities included in any CALEA "solution", despite the prohibitions of CALEA §103(b).

Respectfully submitted,

SBC COMMUNICATIONS INC.

By



James D. Ellis

Robert M. Lynch

Durward D. Dupre

Lucille M. Mates

Frank C. Magill

175 E. Houston, Room 4-H-40

San Antonio, Texas 78205

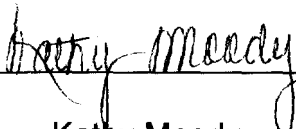
(210) 351-5575

ATTORNEYS FOR SBC
COMMUNICATIONS INC.

February 11, 1998

CERTIFICATE OF SERVICE

I, Kathy Moody, hereby certify that the foregoing "Reply Comments of SBC Communications Inc." have been served on February 11, 1998, to the Parties of Record.


Kathy Moody

February 11, 1998

A. Richard Metzger, Jr.
1919 M Street, N.W. Room 500
Washington, D.C. 20554

ITS
1231 20th Street, NW
Ground Floor
Washington, DC 20036



Office of the Attorney General
Washington, D. C. 20530

01-23-98 05:35P P.03
APPENDIX #1

Mr. Matthew J. Flanigan
President
Telecommunications Industry Association
2500 Wilson Boulevard
Suite 300
Arlington, VA 22201-3834

Dear Mr. Flanigan:

This letter responds to concerns expressed recently by members of the telecommunications industry with respect to the taking (or forbearance) of enforcement actions under the Communications Assistance for Law Enforcement Act (CALEA).

As you know, in enacting CALEA, Congress intended to preserve law enforcement's electronic surveillance capabilities and to prevent those capabilities from being eroded by technological impediments related to advanced telecommunications technologies, services, and features. To that end, Congress also specified that the solutions to overcome these impediments must be implemented within four years of the date of CALEA's enactment. The deadline for carriers to comply with section 103 of CALEA is October 25, 1998.

The Federal Bureau of Investigation (FBI) is working diligently with members of the industry, both individually and collectively, to ensure that the carriers and manufacturers are able to meet the deadline. In those situations where the carrier can foresee that it will not be able to meet the deadline because the manufacturer has yet to develop the solutions, the FBI is prepared to enter into an agreement with the manufacturer of the carrier's equipment wherein both parties (the FBI and a manufacturer) would agree upon the technological requirements and functionality for a specific switch platform (or other non-switch solution) and a reasonable and fair deployment schedule which would include verifiable milestones. In return, the Department will not pursue an enforcement action against the manufacturer or carrier as long as the terms of the agreement are met in the time frames specified. The Department will not pursue enforcement action against any carrier utilizing the switch platform (or non-switch solution) named in the agreement. Finally, the Department will support a carrier's petition to the Federal Communications

Mr. Matthew J. Flanigan
Page 2

- Commission (FCC) for an extension of the compliance date for the equipment named in the agreement and for the length of time specified in the agreement. Where an agreement has been signed, if a dispute arises between the manufacturer and the FBI which cannot be resolved, the manufacturer may appeal the issue directly to the Attorney General or her designate for prompt resolution.

Your continued willingness to work toward solutions which will support law enforcement's electronic surveillance requirements is greatly appreciated.

Sincerely,

Janet Reno



U.S. Department of Justice

APPENDIX #2

FEB -3 1998

Washington, DC 20530

Mr. Geoffrey Feiss
Director, State Relations
United States Telephone Association
1401 H Street, NW, Suite 600
Washington, DC 20005-2136

Dear Mr. Feiss:

This letter confirms discussions held between the Department of Justice (DOJ), the Federal Bureau of Investigation (FBI), and representatives of the telecommunications industry during a January 23, 1998, meeting¹ regarding DOJ's position on the legal status under the Communications Assistance for Law Enforcement Act (CALEA) of the 11 electronic surveillance capabilities (referred to as the 'punch list') that are missing from the current Telecommunications Industry Association (TIA) electronic surveillance standard J-STD-025. Additionally, it confirms the terms and conditions upon which DOJ will forbear bringing enforcement actions against industry members for non-compliance with CALEA.

"Punch List"

DOJ has reviewed the 11 'punch list' capabilities in reference to CALEA, its legislative history, and the underlying electronic surveillance statutes². In addition, DOJ reviewed a memorandum evaluating the 'punch list' under CALEA that was prepared by the Office of General Counsel (OGC) of the FBI. As a result of its

¹Those in attendance at the January 23, 1998, meeting included representatives from the Cellular Telecommunications Industry Association (CTIA), Personal Communications Industry Association (PCIA), Telecommunications Industry Association (TIA), United States Telephone Association (USTA), Bell Atlantic, Department of Justice and the Federal Bureau of Investigation.

² CALEA was enacted to preserve the electronic surveillance capabilities of law enforcement commensurate with the legal authority found in the underlying electronic surveillance statutes, and so that electronic surveillance efforts could be conducted properly pursuant to these statutes.

review, DOJ is providing the following legal opinion: 9 of the 11 capabilities are clearly within the scope of CALEA and the underlying electronic surveillance statutes. These nine capabilities are¹:

- Content of conferenced calls;
- Party Hold, Party Join, Party Drop;
- Access to subject-initiated dialing and signaling;
- Notification Message (in-band and out-of-band signaling);
- Timing to correlate call data and call content;
- Surveillance Status Message;
- Feature Status Message;
- Continuity Check; and
- Post cut-through dialing and signaling.

With respect to the first four capabilities (Content of conferenced calls; Party Hold, Party Join, Party Drop; Access to subject-initiated dialing and signaling; and Notification Message of in-band and out-of-band signaling), DOJ firmly believes that law enforcement's analysis and position regarding these assistance capability requirements satisfy CALEA section 103 requirements. These descriptions are set forth in the response submitted by the FBI² to TIA Committee TR45.2 during the balloting process on standards document SP-3580A.

With respect to the fifth through the ninth capabilities (Timing to correlate call data and call content; Surveillance Status Message; Feature Status Message; Continuity Check; and Post cut-through dialing and signaling), DOJ has also concluded that law enforcement's position satisfies CALEA section 103 requirements. Because of this opinion, discussion between the industry and law enforcement will be required in order to select a mutually acceptable means of delivering the information specified by each capability. Thus, if industry disagrees with law enforcement's proposed delivery method, it must affirmatively propose a meaningful and effective alternative.

Based upon the foregoing analysis, it is DOJ's opinion that TIA interim standard J-STD-025 is failing to include and properly address the nine capabilities listed above. Industry and law enforcement may wish to act in concert to revise the interim standard J-STD-025 to include solutions for each of these missing electronic surveillance capabilities.

¹ See Items 1-7, 9, and 10 of Attachment A.

² The FBI is closely coordinating its efforts with state and local law enforcement representatives across the nation. In this document 'law enforcement' and 'FBI' refer to this partnership and are used interchangeably.

With respect to capability number eight (Standardized Delivery Interface), although a single delivery interface is not mandated by CALEA, DOJ believes that a single, standard interface would be cost effective and of great benefit to both law enforcement and telecommunications carriers. Recent productive discussions with industry have resulted in what DOJ believes is an acceptable compromise, whereby the industry would commit to a limited number of no more than five delivery interfaces. DOJ supports such an agreement.

With respect to capability number 11 (Separated Delivery), DOJ, while recognizing the usefulness of such delivery for the effectiveness of electronic surveillance, nevertheless does not believe that CALEA section 103, or the underlying electronic surveillance statutes, require separated delivery.

Building on the progress made during the final months of 1997, the FBI's CALEA Implementation Section (CIS) will continue to work with solution providers⁵ to reach an agreement on the technical feasibility of all the CALEA capability requirements.

Forbearance

During the January 23, 1998, meeting, the parties discussed the conditions under which DOJ would agree not to pursue enforcement actions against the carrier under section 108 of CALEA with regard to the CALEA mandate that a carrier meet the assistance capability requirements pursuant to CALEA section 103 by October 25, 1998, or against a manufacturer with respect to its obligation under CALEA section 106(b) to make features or modifications available on a "reasonably timely basis." A letter from the Office of the Attorney General, which was provided to all meeting attendees, outlined the basic conditions regarding forbearance:

In those situations where the carrier can foresee that it will not be able to meet the deadline because the manufacturer has yet to develop the solutions, the FBI is prepared to enter into an agreement with the manufacturer of the carrier's equipment wherein both parties (the FBI and a manufacturer) would agree upon the technological requirements and functionality for a specific switch platform (or other non-switch solution) and a reasonable and fair deployment schedule which would include verifiable milestones. In return, DOJ will not pursue an enforcement action against the manufacturer or carrier as long as the terms of the agreement are met in the time frames specified. DOJ

⁵ Solutions providers include not only switch-based manufacturers, and support service providers, but other industry entities that are engaged in the development of network-based and other CALEA-compliant solutions.

will not pursue enforcement action against any carrier utilizing the switch platform (or non-switch solution) named in the agreement.

DOJ, in consultation with the FBI, has further elaborated on the conditions related to forbearance as follows:

Any member of the telecommunications industry seeking forbearance must submit to CIS a statement that identifies the following:

1. The CALEA capability requirements that will be included in its platform or designed into any non-switch-based solution.
2. The projected date by which the platform, or non-switch-based solution, will be made commercially available, the 'commercially available date.'
3. A timeline for design, development, and testing milestones that will be achieved by the manufacturer from the start of the project through the commercially available date, the 'milestone timeline.'
4. A schedule for furnishing information to CIS at each milestone to permit CIS to verify that a milestone has been reached.
5. A list of specific types of information to be provided according to the foregoing schedule.
6. A schedule for providing mutually agreed upon data to CIS from which the Government will be able to determine the fairness and reasonableness of the CALEA solution price.
7. A list of the specific types of price-related data to be provided.

With respect to item 1, the term 'CALEA capability requirements' refers to the functions defined in the TIA interim standard J-STD-025 and the first nine punch list capabilities described earlier in this letter. Law enforcement will work with each solution provider as it produces a technical feasibility study to confirm its understanding of, and ability to meet, the CALEA capability requirements. For those switching platforms, or non-switch-based solutions, on which a capability is technically infeasible, law enforcement will consult with solution providers to assess the possibility of providing effective technical alternatives that will still provide law enforcement with the necessary evidentiary and minimization data sought by the capability.

With respect to item 2, the term 'commercially available date' refers to the date when the platform or non-switch-based solution

will be made available by the solution provider for the immediate purchase and deployment by a carrier. That date shall, in no event, extend beyond the first currently scheduled software generic product release after the October 25, 1998, capability compliance date. With respect to item 3, the term "milestone timeline" refers to a schedule of the necessary design, development, and testing steps to be taken by a solution provider in making a product commercially available. With respect to item 4, a solution provider is expected to include a schedule specifying the time after the completion of each milestone when CIS will be able to verify that the milestone has been reached. With respect to item 5, the specific types of information contained in the affirmative confirmation of the foregoing schedule will include, but not be limited to, draft design documents, feature specification documents, and test results. With respect to item 6, a solution provider is expected to provide a schedule detailing the delivery to CIS of all necessary information for the government to make a determination of the fairness and reasonableness of the price of the solution provider's commercially available CALEA solution. With respect to item 7, the specific types of information contained in the price-related information of the foregoing schedule will include, but not be limited to, market prices of comparable features with similar levels of design, development, and testing effort.

Forbearance for a solution provider, and its carrier customers, will be conditioned upon its ability to provide the above listed items as well as to meet verifiable solution development milestones. A solution provider's failure to meet these milestones will result in the loss of forbearance for the solution provider.

Carrier forbearance ends with the commercial availability of a solution. Switches, or portions of a network, of historical importance to law enforcement for which the government must reimburse the carrier will be identified by CIS. Equipment, facilities, and services installed or deployed after January 1, 1995, will be included in any forbearance until a solution is commercially available. Following solution availability, for those switches or portions of a network not identified by CIS, carriers are expected to follow their normal deployment processes in determining which switches, or portions of their networks, will be upgraded with the CALEA capabilities. Figure 1 illustrates the basic elements of forbearance.

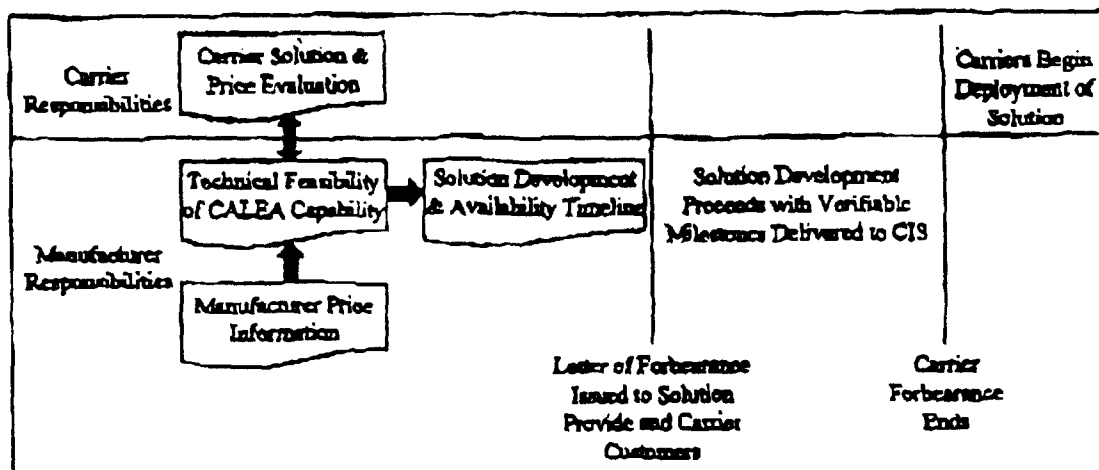


Figure 1: Forbearance

The foregoing forbearance discussion centers on two separate and distinct agreements: Agreements in Principle (AIP) between the FBI and a solution provider, and Cooperative Agreements between the FBI and a carrier.

In an AIP, the FBI and solution providers agree that solution providers have complied with the seven criteria listed above, including a feasibility analysis and pricing information for CALEA capability requirements. The feasibility analysis and pricing information will allow the government to finalize its position regarding the standard, extension of the compliance dates, forbearance, etc. The FBI, in consultation with law enforcement, will not be in a position to make critical determinations until the information described in the above seven criteria has been provided.

Currently many versions of draft AIPs are circulating, both FBI- and industry-generated, and some are more comprehensive than is presently warranted. Some of the AIPs in circulation were derived from an AIP drafted by TIA. The FBI hopes to meet with TIA during the week of February 2, 1998, to discuss the proposed AIP. The results of these discussions will then be disseminated to TIA's membership and any other interested solution provider.

The Cooperative Agreement, on the other hand, is the contractual vehicle whereby telecommunications carriers will receive reimbursement for their eligible CALEA costs. Cooperative Agreements may be executed for different purposes at different stages of CALEA implementation. For example, an initial round of Cooperative Agreement negotiations is taking place to establish contractual vehicles whereby carriers selected to support specific solution providers with the feasibility analyses and pricing information may receive reimbursement for assisting in